الباب الثانى

قضايا الكمبيوتر :-
الأمن - الخصوصية - الأخلاقيات

COMPUTER ISSUES :-
Security , Privacy , Ethics

بعد فترة وجيزة من تعاملك مع الكمبيوتر ستشعر بأنه كل شئ فيه محسوس ويسهل إدراكه وتعريفه : الجهاز بمكوناته المختلفة والبرامج بأنواعها المتباينة والشبكات التى تربط الأجهزة ببعضها البعض .. ولكن هناك اعتبارات أخرى تؤثر تأثيرا بالغا على مناخ عمل المنظومة الكمبيوترية ويصعب تقنينها ووضع إطار واضح لها .. هذه الاعتبارات تمثل فى الواقع قضايا جديدة جديرة بالبحث ، ويمكن تقسيمها إلى فئات ثلاث :

- اعتبارات الأمن
- اعتبارات الخصوصية
- الاعتبارات الأخلاقية

فاذا احتفظت ببيانات تهمك فى ملف قاعدة بيانات واكتشفت أنه هناك من تسلل إلى جهازك وعبث بهذا الملف أو دمره بالكامل ، فاعلم أنه بياناتك لم تكن فى أمن .. واذا تبادلت رسائل سرية بالبريد

الالكتروني مع أحد زملائك في العمل وعلمت أنه رئيسك قد اطلع عليها ، فستضرر حتما من انتهاك خصوصيتك .. وإذا أعرت صديقا لك برنامجا من تصميمك وفوجئت بأنه طبع نسخا منه وباعها لحسابه الخاص ، فصديقك تغير قضية أخلاقية .. و القصص - كما سنرى في هذا الباب - كثيرة وخطيرة وتعتبر آثارا سلبية لعصر الكمبيوتر - عصر المعلومات المميكنة و الاتصالات التي لا تحدها حدود .

٢-١ جرائم الكمبيوتر
(Computer crimes)

الكمبيوتر - على عظمة إمكانياته - مجرد آلة تطيع أوامرك طاعة عمياء طالما أنك تتعامل معها بلغتها ونظام تشغيلها .. وكلما تعمقت في فهم دقائق آلة الكمبيوتر كلما زادت مهارتك في توظيفها وتوجيهها كيفما تريد ... والفهم المتعمق هنا سلاح ذو حدين ، فقد يدفع إلى المنفعة والخير - وهذا هو الهدف - وقد يحرّض على الإثم والشر .. الكهرباء - مثلا - تخلق بيئة مشابهة : فهي تقدم للبشرية أجل الخدمات ، وهي ذاتها التي تصعق إنسانا في جريمة قتل بشعة .

وللتعرف على طبيعة جرائم الكمبيوتر نذكر

٢-٤ أمن الكمبيوتر (Computer security)

رأينا- من استعراضنا جرائم الكمبيوتر - كيف أنه العمل الكمبيوترى فى أمس الحاجة إلى خطط أمنية مدروسة لمواجهة ضربات "تكنولوجية" ماكرة يتفتق عنها كل يوم العقل البشرى متضامنا مع العقل الالكترونى.

وتعبير "أمن الكمبيوتر" كان يعنى فى الماضى شيئا واحدا محددا: أمن الجهاز نفسه خوفا من سرقته أو إتلافه، فكانت الاحتياطات تقتصر على إغلاق الأبواب وتشديد الحراسة.. وكلنا الأبواب المغلقة المحروسة لم تعد مجدية فى زمن يمد فيه الهارد "يده" أميالا وأميالا ليصل إلى البيانات فى قواعدها داخل الأجهزة، وهو بعيد تماما عن العيون والآذان يدبر بهدوء وينفذ بتأن.

لذلك تولد لدى مديرى الشركات إحساس فائق بضرورة توفير نظم وأدوات أمن على مستوى عال، وأصبحوا يتسابقون لشراء كل ما هو حديث ومتقدم فى هذا المجال.

فما هو "أمن الكمبيوتر" اليوم؟ إنه نظام محكم لحماية أجهزة وبرامج وبيانات المنظومة الكمبيوترية للمنشأة من حوادث السرقة أو الإتلاف أو التدمير أو التجسس، وكذلك حمايتها من أخطار الكوارث الطبيعية وغير الطبيعية كالزلازل والفيضانات والحرائق والعمليات الإرهابية وغيرها.

٢-٤-١ تصريح الدخول إلى منظومة الكمبيوتر (Allowing access to computer system)

من العناصر الأولية الرئيسة للنظام الأمن الكمبيوتري احتواؤه على وسائل التعرّف على الأفراد المصرح لهم (Authorized persons) بالدخول إلى المنظومة الكمبيوترية واستخدام إمكانياتها والتعامل مع برامجها وبياناتها، وسنسمي هؤلاء الأفراد "المفوّضين".. وكذلك التعرّف على الأفراد غير المصرح لهم (Unauthorized persons) بالدخول إلى المنظومة الكمبيوترية وسنسميهم "غير المفوّضين".

فاذا كنت مفوّضا من نظامه بعملك، فكيف يمكنك إثبات ذلك؟ توجد على وجه العموم أربعة أساليب:

(١) الاثبات بما معك
(٢) الاثبات بما تعرف
(٣) الاثبات بما تفعل
(٤) الاثبات بتحقيقه شخصيتك

(١) الاثبات بما معك (What you have)

قد يكون معك مفتاح أو شارة أو كارت مغناطيسي أو أي وسيلة أخرى من هذا القبيل تستطيع بها أن تدخل من باب حجرة الكمبيوتر أو أنك تستخدم جهازا

مغلقا .. فعلى سبيل المثال يمكنك كارت ذو شريط ممغنط من الوصول الى حسابك فى أحد البنوك والصرف منه عن طريق خزينة مبرمجة مثبتة بعيدًا عن البنك .

وفى الآونة الأخيرة شاع استخدام وسيلة مبتكرة تسمى "الشارة النشطة" (Active badge) وهى عبارة عن كارت مزوّد ببوائر الكترونية دقيقة يضعه الشخص على صدره طوال فترة تواجده بالعمل ، فيرسل الكارت أشعة تحت حمراء (Infrared) ليستقبلها عدد كبير من الأجهزة الصغيرة الحساسة (Sensors) المركبة فى أنحاء متفرقة من المبنى .. وبواسطة هذا النظام يتسنى تحديد المكان الذى يذهب إليه الشخص فى أى لحظة ، ويسهل بذلك ضبط غير المفوّضين الذين يحاولون الدخول الى مواقع عمل الكمبيوتر .

وتثير الشارات النشطة جدلا واسعا ، إذ يعتبرها الكثيرون قيدا على حريتهم ودليلا على عدم ثقة الادارة فى أمانتهم .

(٢) الاثبات بما تعرف (What you know)

الوسائل المعتادة لأسلوب الاثبات بما تعرف هى كلمات السر (Passwords) و أرقام التمييز (Identification numbers) .. ولاشك

أنك شاهدت - مثلا - الأقفال السرية (Cipher locks) التي لا تفتح إلا بمجموعة أرقام معينة .. لاحظ أيضا أنك لا تستطيع استخدام خزينة البنك المبرمجة إلا بواسطة رقم مميز يخصك (بالإضافة إلى الكارت ذى الشريط المغنط الذى أشرنا إليه سابقا) .

(٣) الإثبات بما تفعل (What you do)

يعتمد هذا الأسلوب على توقيع الشخص (Person's signature) .. ورغم أن تقليد التوقيعات ليس سهلا إلا أنه التزوير دائما وارد .. وفى الحقيقة إذا كانت نظام التوقيعات قد أثبت نجاحا فى العلاقات البشرية ، فإنه ينبغى ألا يعوّل عليه كثيرا فى التعاملات الآلية .

(٤) الإثبات بتحقيق شخصيتك (Who you are)

يستحوذ هذا الأسلوب حاليا على اهتمام كثير من المشتغلين بأمن الكمبيوتر ، ففيه تطبيق نظريات علم "القياسات الحيوية" (Biometrics) الذى يختص بعمليات قياس المواصفات الجسدية للإنسان. وأشهر وسيلة هنا هى بصمات الأصابع

(Finger-prints) ، وقد تبدو للوهلة الأولى وسيلة قديمة وغير مناسبة .. ولكنها تخلصت الآن من "الحبر والختامة"، وأصبح كل المطلوب من الشخص مجرد وضع إصبعه لثوانٍ معدودة في ماكينة صغيرة لتحقيق الشخصية.

والوسيلة الثانية تعتمد على تمييز الصوت (Voice recognition) .. فلكل إنسان نبرات وخصائص صوتية خاصة به - دون غيره - ويمكن رصدها بأجهزة دقيقة.

والوسيلة الثالثة - الحديثة والشيقة - تقوم على تمييز شبكية العين (Retina) .. فقد ثبت أن شبكية عين كل إنسان تحتوي على ملايين من الخلايا الحساسة للضوء مرتبة في نسق معين لا يتكرر مع أي إنسان آخر .. فإذا نظر الشخص بعينه داخل جهاز صغير مصمم لهذا الغرض، أمكن التحقق من شخصيته على أساس نمط شبكية عينه.

٢-٤-٢ خطة مواجهة الكوارث
(Disaster recovery plan)

يجب أن تعد المؤسسة - التي تحافظ على كيانها وعملها وسمعتها - خطة لمواجهة الكوارث التي قد تصيبها فجأة بفعل فاعل أو قضاءً وقدرا.

ففي إيطاليا، وعلى مدار سنة كاملة، قامت

أو إتلافها عمداً.

ورغم أهمية إجراءات أمن الأجهزة، إلا أنه فقدان جهاز - في حد ذاته - لا يمثل مشكلة خطيرة للمؤسسة، إذ أن الخسارة المادية يسهل تعويضها عن طريق شركات التأمين ويمكن في جميع الأحوال شراء جهاز جديد يحل محل الجهاز المفقود.. ولكن المشكلة الحقيقية تتمثل في الوقت الذي سيمضي قبل أن تتمكن المؤسسة من تدبير الأجهزة البديلة، فأي جهاز يتوقف عن العمل يؤثر بالسلب على كفاءة العمل ككل.. ولك أن تعلم أن مؤسسات كثيرة (كالبنوك ومراكز المعلومات) قد تضطر لإغلاق أبوابها وإشهار إفلاسها في غضون أيام بسبب خروج بعض كمبيوتراتها من منظومة العمل.

٢-٤-٤ أمن البرامج (Software security)

من بديهيات العمل الكمبيوتري أن تحتفظ المؤسسة بنسخ بديلة (Backup copies) لجميع برامجها.. ويجب أن يؤخذ هذا الاحتياط مأخذ الجد دائماً حتى تنفذ النسخة البديلة الموقف في حالة فقدان البرنامج الأصلي.

ويطرح أمن البرامج قضية "ملكية البرنامج" (Program ownership): فإذا صمم أحد المبرمجين برنامجاً لحساب شركة معينة، فمن يصبح المالك الحقيقي للبرنامج؟ المبرمج أم الشركة؟ ثم كيف يكون

التصرف إذا أخذ المبرمج نسخة من برامجه معه وهو ينتقل من شركة إلى شركة ؟ هل يمنعه أحد ؟ هل يردعه قانونه ؟

وللإجابة على هذه الأسئلة نقول : إذا كان مصمم البرنامج أحد العاملين بالشركة ، فتؤول ملكية البرنامج إلى الشركة ، وليس من حق المبرمج في هذه الحالة أن يأخذ نسخة من البرنامج معه عند انتقاله للعمل بشركة أخرى .. أما إذا كان المبرمج مستشارا فقط للشركة ، فيجب أن ينص صراحة في العقد المبرم بين الطرفين على من سيصير مالك البرنامج — المستشار أم الشركة ؟ وإذا لم يذكر هذا النص في العقد (أو إذا لم يكن هناك عقد على الإطلاق) فإن الطرفين - عند اختلافهما - سيدخلان متاهات مضنية وعقيمة .

وتمثل عمليات نسخ برامج الكمبيوتر بدون تصريح مشكلة عامة مؤرقة لم يظهر لها علاج ناجع حتى وقتنا هذا .. في الولايات المتحدة أصدرت المحكمة الأمريكية العليا قرار "حقوق تأليف البرامج" بحيث لا يسمح بنسخ أي برنامج إلا بموافقة كتابية صريحة من مالك البرنامج .. وفي مصر بدأت شركات البرمجة تلجأ إلى القضاء بعد أن تكبدت خسائر جسيمة من جراء نسخ برامجها بدون تصريح .

ورغم ذلك فواقع الحال يقول إن البرامج لا زالت تنسخ على مرأى وسمع من الجميع مثلما تنسخ شرائط الأغاني والموسيقى على أجهزة التسجيل .. والقضية مستمرة وساخنة ، وسنعود إليها عند مناقشتنا للاعتبارات

عصابة مسلحة بتفجير عشرة مراكز حيوية للكمبيوتر.
وفى نيويورك انقطع التيار الكهربائى لمدة ثلاثة أيام وتوقفت عمليات الكمبيوتر وشلت مواقع العمل وحركات الطيران والنقل فى مناطق شاسعة بالولايات المتحدة.

وفى كاليفورنيا هاجم إرهابيون قاعدة فاندنبرج (Vandenberg) الجوية، ودمروا ضخمة أجهزة كمبيوتر من النوع الكبير (Mainframe) ولاذوا بالفرار بعد أن تركوا وراءهم باقة من زهور البانسيه (Pansy) وعلبة حلويات ورسالة تقول "نتمنى لكم يوما سعيدا".

ناهيك عن الزلازل والبراكين والفيضانات والأعاصير والحرائق التى تلحق أفدح الخسائر بالمؤسسة وقد تزيلها من على سطح الأرض.

وفطة مواجهة الكوارث تتضمن كيفية التصرف عند مداهمة الكارثة للمؤسسة، بحيث يتم استعادة قدرات عمل المنظومة الكمبيوترية للإستمرار فى الجو المعتاد - أو شبه المعتاد - لمزاولة سائر الأنشطة .. وهناك أكثر من طريقة :

● فقد تختار المؤسسة أن تعود مؤقتا إلى الخدمة اليدوية والملفات الورقية التى يكون قد سبق إعدادها كبديل للملفات الالكترونية وقت الحاجة .. ولكن العاملين والعملاء سيعانون من متاعب ليست هينة فى فترة

توقف الخدمة الآلية.

- وقد تشترى المؤسسة وقت عمل على الكمبيوتر الخاصة بمكاتب الخدمة (Service bureaus) لمواصلة أعمالها لحين زوال آثار الكارثة .. وإذا كانت هذه المكاتب لا توجد في الغالب إلا بالعواصم والمدن الكبيرة.
- وأحيانا تعقد مؤسستان أو أكثر في منطقة جغرافية معينة "اتفاقية عون متبادل" (Mutual aid pact)، فإذا تعطل العمل في إحدى المؤسسات استعانت بإمكانيات المؤسسة الأخرى بناءً على الاتفاقية .. بيد أن فائدة مثل هذه الاتفاقيات قد تتضاءل أو تنعدم إذا ما حلت الكارثة بالمنطقة كلها وباتت المؤسسات جميعا تستغيث.
- وفي حالة الشركات والبنوك ذات الأفرع المنتشرة في مختلف أقطار العالم والتي تعتمد كلية على المنظومات الكمبيوترية العملاقة وتعتبر سلامة هذه المنظومات بالنسبة لها مسألة حياة أو موت، فيتم تكوين "اتحاد" فيما بين مجموعة شركات متضامنة يسمى Consortium يتولى إقامة منظومة كمبيوترية متكاملة بديلة للجوء إليها فورا عند الخطر .. وتتكلف هذه المنظومة بالطبع مبالغ ضخمة لبنائها والحفاظ عليها واختبار كفاءتها بصفة دورية.

ومع ضخامة مزاعم تلك المنظومة نوعا ما

المواقع : الموقع الساخن (Hot site) وهو مركز مجهز تجهيزا كاملا بكل متطلبات العمل من كمبيوترات وبرامج وخطوط اتصال ووسائل سيطرة وأمن وخلافه، والموقع البارد (Cold site) وهو مركز خال مهيأ لأن تنتقل اليه الشركة وتمارس كافة أعمالها ولكن بعد تركيب الأجهزة والمعدات اللازمة.

وتقوم كل مؤسسة باعداد خطتها لمواجهة الكوارث مبكرا، كما تتيح للعاملين فرص التدريب عليها بيئة الحية والحية لكن يجيدوا تنفيذها إذا دهم ناقوس الخطر.

وتنبني الخطة على أنه كل شيء - فيما عدا الأجهزة - يجب حفظه في مكان بديل آمن بعيد عن مقر المؤسسة الأصلي .. فيتم حفظ البرامج وملفات البيانات الرئيسية وسجلات أسماء البرامج وسجلات مواصفات الأجهزة ونسخ من نظم التشغيل وصورة من خطة مواجهة الكوارث ... الخ .. كما تغطي الخطة النقاط الأساسية التالية.

(١) الأولويات (Priorities)

تضع الخطة قائمة أولويات للبرامج والبيانات التي ينبغي المحافظة عليها وتذليل كل العقبات للوصول اليها دائما.. فالبنك مثلا تهمه ملفات أرصدة العملاء بدرجة تفوقه بمراحل كثيرة جداول أجازات العاملين.

(٢) احتياجات الأفراد (Personnel requirements)

توضح الخطة كيفية الاتصال بالعاملين لتوعيتهم بحجم الخطر

الذى يهدد المؤسسة وإخبارهم بالتغييرات التى ستطرأ على أماكن العمل ونظمه ووسائله فى الظروف الجديدة الصعبة.

(٣) احتياجات الأجهزة (Equipment requirements)

تحدد الخطة ما يحتاجه العمل من أجهزة وبرامج ومعدات وأماكن الحصول عليها وطرق تركيبها وتشغيلها فى الأماكن البديلة المقترحة .. خليت كل مؤسسة عضوا فى "اتحاد" قوى وقادرة على اقتناء "موقع ساخن" مستعد لاستضافتها فى أى لحظة.

(٤) استقبال وتوزيع البيانات

(Capture and distribution)

فى هذا الجزء من الخطة تحدد طرق إدخال البيانات الى المنظومة الكمبيوترية البديلة واستعادة هذه البيانات (أو أجزاء منها) وتوزيعها حسب مقتضيات العمل فى بيئة مختلفة وأجواء ضاغطة.

٢-٤-٣ أمن الأجهزة (Hardware security)

على ضوء ما سبق يمكننا القول بأن أمن المنظومة الكمبيوترية يتضمن أمن الأجهزة وأمن البرامج وأمن البيانات .. ونبدأ بالقاء نظرة على أمن الأجهزة.

أجهزة الكمبيوتر وملحقاتها - مثلها فى ذلك مثل أى معدات ذات قيمة - يجب توفير الأمن والحماية لها بحيث لا تفاجأ المؤسسة بسرقة أحد الأجهزة

الأخلاقية بعد قليل .

٢-٤-٥ أمن البيانات (Data security)

تحتل البيانات المحوسبة اليوم على رأس قائمة المقتنيات الثمينة للمؤسسة ، ومن هنا يبرز الدور الحيوي لأمن البيانات والذي يتجلى في المجالات الخمسة الآتية :

(١) رسم سياسة واضحة وحاسمة في شأن التعامل مع البيانات يكون محورها : حماية البيانات وكل ما يتعلق بها من معلومات من أضرار الوصول إليها بدون تصريح ومن أخطار تزييفها أو تدميرها.

(٢) استخدام كلمات السر (Passwords) وغيرها من طرق الحماية لقصر التعامل مع البيانات على الأشخاص المصرح لهم بذلك .

(٣) تخطيط احتياطات الأمن في المراحل الأولى لتصميم المنظومة الكمبيوترية .. فهذا أفضل وأيسر من التفكير في مثل هذه الاحتياطات بعد اكتمال بناء المنظومة .

(٤) دراسة القوانين والتشريعات التي تخص الأمن بوجه عام ، والتركيز على رصد وبلورة المشكلات الخاصة بأمن البيانات والمطالبة بتقنين حلول لها .

(٥) القيام بعمليات صيانة دورية لسجلات البيانات

التاريخية القيمة حتى لاتتلف بتأثير طول فترة التخزين .

وهناك خطوات يمكن اتخاذها للمساعدة فى وضع سياسة أمن البيانات موضع التنفيذ ، نذكر منها :

(أ) كلمات السر (Passwords)

ذكرنا أننا نستخدم كلمات السر لقصر التعامل مع البيانات على الأشخاص المصرح لهم بذلك .. وكلمة السر عبارة عن كلمة أو رقم أو خليط من الاثنين ، ويتم إدخالها إلى الكمبيوتر عن طريق لوحة المفاتيح .

ويفضل أن تتجزأ البيانات إلى فئات بحيث تحدد لكل فئة كلمة سر معينة ، وبذلك يكون التصريح المعطى للشخص يختص بفئة بيانات واحدة دون الفئات الأخرى .. كما ينبغى أن تتغير كلمات السر من وقت لآخر .

(ب) وسائل التحكم الداخلى (Internal controls)

يمكن أن تكون المنظومة الكمبيوترية مزودة بمكونات داخلية تعمل ذاتيا لمراقبة حركة التعامل مع البيانات ، فيتم مثلا توظيف ملف لتسجيل كل عمليات الوصول أو محاولة الوصول الى البيانات .

كما يمكن أن يبنى نظام التشغيل (Operating system) بطريقة تفرض ضوابط فنية على عمليات الوصول الى البيانات .. فى إحدى هذه الطرق يقارن رقم المستخدم برقم البيانات فيظهر ما اذا كان الشخص

مصرحاله بالتعامل مع هذه البيانات أم أنه يتحايل للوصول إليها في الخفاء .. وفي طريقة أخرى يتم تخزين "سيرة" كل مستخدم (User profile) التي تضم معلومات كاملة عنه بما فيها فئات البيانات المصرح له بالتعامل معها ، ويرجع إلى هذه المعلومات كلما اقتضى الأمر .

(هـ) فصل الأعمال الوظيفية

(Separation of employee functions)

يجب أن تفصل الوظائف المتعلقة بالعمل الكمبيوتري عن بعضها البعض كلما أمكن ذلك .. فالمبرمج مثلا ينبغي ألا يكون مسئولا في نفس الوقت عن تشغيل البرامج ، لأنه جمع شخص واحد بين العمليين لا يعطيه فرصة كتابة برامج غير مصرح بها فحسب ، وإنما تمنحه أيضا إمكانيات تجربة هذه البرامج وتشغيلها والحصول منها على المعلومات التي يسعى إليها .. وفصل الوظائف إجراء مألوف ومطبق في الأعمال العادية ، فلا نجد مثلا موظفا واحدا مسئولا عن أعمال تقدير المبالغ المستحقة وتحرير الشيكات اللازمة لها وتوقيع هذه الشيكات وختمها بشعار الجمهورية ، بل يعين أكثر من موظف للقيام بهذه الأعمال تتابعيا فيكون كل واحد منهم مراجعا لعمل زميله الذي يسبقه .

وثمة نقطة أخرى تستحق التنويه : كثيرا ما نصادف موظفا مواظبا على عمله لأقصى درجة ، لا يتأخر ولا يتغيب ولا يتشاجر ولا يتذمر ولا يأخذ أي

نوع من الأجازات .. ورغم هذه المثالية إلا أنه قد يكون متأثرا - بقصد أو بدون قصد - بقدر كبير من المعلومات الهامة والأعلم للإدارة بذلك .. من هنا يحث مديرو الشركات الموظفين دائما على القيام بأجازاتهم لكي يتبين ما يحوزة كل موظف من معلومات ومدى أهميتها .. وخير للإدارة أن تكتشف هذه الخبايا و الموظف في أجازة قصيرة من أن تكتشفها بعد انتقال الموظف للعمل بشركة أخرى.

(ى) مراجعة الحسابات (Auditor check)

يعمل لدى معظم الشركات عدد من مراجعي الحسابات لضبط الدفاتر المالية ويدخل في نطاق عملهم مراجعة كافة البرامج و البيانات .. وكاجراء أمني للملفات يكلف هؤلاء المراجعون أيضا بحصر الأشخاص الذين تعاملوا مع ملفات البيانات في الفترات المعروف أنه أحدا لا يهتم خلالها بالاطلاع على أي بيانات ، وكذلك البحث وسط الملفات عن أي أرقام شاذة أو سجلات غير مكتملة .. فقد يؤدي ذلك الى اكتشاف عملية تزييف أو تدمير.

ومن ناحية أخرى توجد برامج جاهزة لمراجعة الحسابات (Audit software) يمكن بواسطتها اختبار صحة ودقة عمليات المنظومة ومخرجاتها .. وتلعب هذه البرامج دورا في تعزيز الاحتياطات الأمنية إذ تتيح للمراجعين إمكانية أداء عملهم بدون اللجوء

الى مبرمجى الشركة .

(هـ) اختبار العاملين الجدد (Applicant screening)

فى نظام الأمن الكمبيوترى ينظر الى العنصر البشرى على أنه نقطة ضعف النظام ، فالكمبيوتر لايفعل شيئا - مفيدا أو ضارا - إلا بأوامر من الانسان .. وعليه يجب تحرى الدقة المتناهية عند اختيار الأشخاص المتقدمين لوظائف شاغرة بالشركة حتى يتسنى اختيار الشخص الأمين ذى السمعة الطيبة واستبعاد كل من يحوم حوله شك .

(و) تأمين صناديق النفايات (Secured waste)

لاينتبه كثيرون لصناديق النفايات ، ولكذلك تعتبر مصدر خطورة فى سياسة أمن البيانات [راجع شكل (٢-١)] .. فصور المستندات و المطبوعات وشرائط الطبع التى تلقى بلامبالاة فى هذه الصناديق قد تحتوى على معلومات محظور خروجها من الشركة أو مقصور التعامل بها على أصحاب التصاريح الخاصة .. لذلك يجب تأمين صناديق النفايات باستخدام الأنواع محكمة القفل وهرمها محتوياتها أولا بأول تحت إشراف مسئولى الشركة .

٢-٥ فيروس الكمبيوتر (Computer virus)

الفيروسات - فى المصطلحات الطبية - جراثيم صغيرة

تتكاثر فى الخلايا الحية وتجلب الأمراض للجسم .. وفيروس الكمبيوتر يهاجم بطريقة مماثلة الأجهزة والبرامج والبيانات وتنجم عنه علل كثيرة تتراوح من إرسال عبارات غريبة واصدار أصوات مزعجة الى تدمير الملفات و إصابة الذاكرة بالشلل التام .. وتحمل كلمة فيروس معانى الخوف و التهديد و الارتباك للعاملين فى الحقل الكمبيوترى.. ويكفى أن نقول إن الفيروسات الكمبيوترية تكلف اقتصاد الولايات المتحدة أكثر من ٢ مليار دولار سنويا.

فما هو هذا الفيروس ؟ إنه برنامج (مجموعة من الأوامر الموجهة إلى الكمبيوتر) يكتبه صاحبه لغرض شرير فى نفسه.. وبرنامج الفيروس - كما يدل الاسم - برنامج مُعْدٍ : فهو يستقر فى الذاكرة ثم ينقل عدواه الى أى برنامج يقترب منه فى ذات الذاكرة .. وعندما يصاب البرنامج الجديد يصبح بدوره حاملا للفيروس ، وبهذه الطريقة تسرى العدوى من برنامج الى برنامج.. ويتفشى الوباء.

والفيروسات المنتشرة حاليا تفوق الحصر ، ونذكر على سبيل المثال :

- **فيروس "يانكى دودل" (Yankee Doodle)**

عندما يصيب فيروس يانكى دودل (الاسم مأخوذ من أغنية أطفال شهيرة) إحدى المنظومات ، فانه يجعل الكمبيوتر يصدر ضوضاء مزعجة فى تمام الساعة الخامسة مساءً كل ثمانية أيام.

• فيروس "القدس ب" (Jerusalem B)

ينشط هذا الفيروس طوال يوم الجمعة الموافق ١٣ من الشهر الميلادى .. ويأخذ فى محو بيانات أى ملف يتم تحميله فى الذاكرة من أقراص التخزين .

• فيروس "الشلال" (Cascade)

يصيب هذا الفيروس نظام التشغيل (Operating system) .. ويتسبب فى عدم إتمام كتابة النصوص والتعليمات ، إذ تسقط بعض الحروف من الأسطر بصورة عشوائية وتتراكم فى قاع شاشة العرض .

وبالاضافة إلى الفيروسات توجد الديدان (Worms) .. ودودة الكمبيوتر هى برنامج - مثل برنامج الفيروس - ولكنه ينتقل من كمبيوتر الى كمبيوتر عبر شبكة كمبيوترية .. وتزرع الدودة نفسها على هيئة ملف منفصل فى أقراص التخزين المستهدفة .

ومن أخطر البرامج الدودية ذلك البرنامج الذى خططه طالب يدعى "روبرت موريس" (Robert Morris) بجامعة "كورنل" (Cornell) الأمريكية وتمكن من حقنه فى شبكة البريد الالكترونى ، وطاف هذا البرنامج بطول وعرض الولايات المتحدة وشل عمل آلاف الكمبيوترات .. فقد كانت الدودة تتكاثر داخل الشبكة بطريقة استعصت على السيطرة ، وكانت تزاحم ذاكرة الكمبيوتر المصاب وتفتك برا جزءا جزءا حتى يزار وسط التخزين بالكامل .

والآن ألا توجد طريقة نتقى بها شر الڤيروسات والديدان ؟! الحقيقة أنه المعركة طويلة والضربات قوية وفى كل يوم نسمع عجبا .. ولكننا نلفت الأنظار لما يلى :

• أكثر الطرق سهولة لانتقال الڤيروس من كمبيوتر الى كمبيوتر هى "الديسكيتات" (Diskettes) .. لذلك يحظر دخول ديسكيتات من الخارج الى حجرة الكمبيوتر ، ويراعى دائما أن تستخدم ديسكيتات جديدة واردة فى أغلفتها الأصلية .

• تنتشر الڤيروسات أيضا عن طريق تبادل برامج الألعاب الكمبيوترية (Computer games) .. فالمبرمج يدس مجموعة تعليمات ڤيروسية فى برنامج اللعبة و"يهديه" بدون مقابل لعدد من معارفه الذين يقومون بتحميله فى ذواكر كمبيوتراتهم .. ومن هنا تبدأ العدوى فى الانتقال الى البرامج السليمة التى تدخل لكل ذاكرة .

• يجب الحذر من البرامج التى تأتى لك بدون توقع من شركات غير معروفة ولم يسبق لك التعامل معها .

• توجد برامج للكشف عن الڤيروس
(Virus-scanning software)
وهذه يجب استخدامها للتحقق من سلامة أى ملف

قبل تحميله على الأقراص الصلبة (Hard disks).

• إذا استعار واحد من أصدقائك ديسكيتات خاصة بك وأعادها إليك، فيجب أن تتحقق من سلامتها بواسطة برامج الكشف عن الفيروس قبل أن تستخدمها مرة ثانية.

• توجد برامج لمحاربة الفيروس
(Antivirus software)
وهي برامج مصممة خصيصا لإيقاف انتشار الفيروس، ومحاصرته ومحاولة القضاء عليه.. ويمكن استخدام هذه البرامج أيضا للتحقق من سلامة القرص الصلب في كل مرة يبدأ فيها العمل على الكمبيوتر أو بصفة دورية حسبما يتراءى لك.

٢-٦ أمن شبكات الكمبيوتر
(Computer network security)

تطرح شبكات الكمبيوتر مشكلات أمنية معقدة وذات طبيعة خاصة، فالشبكة مترامية الأطراف، ومجالات العمل عليها واسعة ومتعددة، وعدد مستخدميها يفوق الحصر، والاتصالات والارتباطات تتم من على بعد كبير في أجواء غامضة.
فما هي مقومات سياسة الأمن تحت هذه الظروف؟
في البداية يوجه الاهتمام الى نظم تشغيل الشبكة (Network operating systems) حيث تؤخذ احتياطات

أمنية أساسية مثل ضرورة التحقق من شخصية المستخدم، عن طريق كلمات السر مثلاً.

وفي معظم الشبكات توجد إمكانية التحكم للمستخدمين بالاستفادة من خدمات معينة دون خدمات أخرى، فقد يسمح لجميع العاملين باحدى الشركات باستخدام برامج تنسيق الكلمات (Word processing) بينما يقتصر الاطلاع على ملفات إنتاج وأرباح الشركة على عدد محدود من المسئولين.. كما توجد إمكانية وضع حد أقصى لعدد مرات استخدام ملفات البيانات، فيتم رصد أسماء الملفات وعدد المرات الفعلية التي تعامل فيها المستخدم مع كل ملف.

وتم التوصل إلى أسلوب فني لدعم أمن الشبكات يسمى "حائط النيران" (Firewall).. وحائط النيران هذا كمبيوتر معين يتم تخصيصه - من بين كمبيوترات شبكة الشركة - للاتصال بمفرده بالعالم الخارجي (Outside world)، بدلاً من الاتصالات الخارجية المفتوحة التي يمكن أن تتم مع كمبيوترات الشبكة المتعددة ويصعب مراقبتها وإحكام السيطرة الأمنية عليها.

ومن مهام حائط النيران أيضا الاحتفاظ بقائمة أرقام تليفونات الجهات الخارجية التي توافقه الشركة لها على التعامل مع شبكتها.. فتتصل الجهة أولا بكمبيوتر حائط النيران وتطلب الوصول الى الشبكة.. فاذا كان رقم تليفون هذه الجهة ضمن القائمة التي يحتفظ بها الكمبيوتر، يعيد الكمبيوتر الاتصال بالجهة ويخبرها بأن وصولها للشبكة

متاح ، ومن هنا يبدأ الاتصال .. أما إذا لم يكن رقم تليفون الجهة الطالبة ضمن القائمة فلا يعيد الكمبيوتر الاتصال بها مانعا بذلك أى تعامل لها مع الشبكة .. لاحظ أنه لا خوف من معرفة الجهة الخارجية (غير المرغوب فيها) لرقم تليفون حائط الميراه ، فاتمام عمليات الاتصال بالشبكة مرهون بمعرفة حائط الميراه لأرقام تليفونات الجهات الخارجية .

وبالاضافة الى فرض الرقابة على الاتصالات التى تأتى للشبكة من الخارج ، ينبغى على الشركة أن تولى اهتماما لمشكلة التدخل غير المشروع فى البيانات وهى لا زالت على الطريق أثناء انتقالها من مكان الى مكان .. فهناك لصوص وجواسيس يلجأون لارتكاب جرائمهم الكمبيوترية على طريقة قطّاع الطرق .. ويمكن توفير الحماية للبيانات فى هذه الحالة بواسطة عمليات "التشفير" (Encryption) .. فتكتب البيانات طبقا لشفرة خاصة لا يعرفها إلّا المرسل لها عند بداية خط الاتصال على الشبكة ولا يقدر على فك رموزها إلّا المستقبل لها عند طرف الاتصال الآخر .. وقد تم تصميم شفرات قياسية لهذا الغرض منها "المواصفة القياسية لتشفير البيانات" [Data Encryption Standard (DES)] التى اعتمدها "المعهد القومى الأمريكى للمواصفات" وتستخدم الآن على نطاق واسع .

وتوجد برامج تشفير (Encryption software) كذلك للكمبيوترات الشخصية حيث تستخدم لتشفير الملفات

وإغلاقه لوحات المفاتيح وحماية كلمات السر .

٢-٧ اعتبارات الخصوصية (Privacy)

فى حياتنا اليومية نضطر لاعطاء بيانات ومعلومات تخصنا الى العديد من الجهات والأفراد .. فما أكثر الاستمارات التى نملؤها لاستخراج البطاقات الشخصية أو العائلية ، تحرير عقود الزواج ، الالتحاق بعمل جديد ، الاشتراك فى نادٍ رياضى ، تسديد الضرائب ، أداء الخدمة العسكرية ، دخول مستشفى للعلاج ، رفع دعوى قضائية ، المطالبة بمعاش أو تأمين اجتماعى ، السفر للخارج ، شراء بضائع عن طريق البريد ، المشاركة فى عمليات التعداد وقياس الرأى العام ... الخ .

وقد لا نستطيع حصر الطرق التى يتم بها جمع بيانات عن المواطنين ، ولكننا نستطيع أن نقول بكل تأكيد أين تذهب هذه البيانات : إلى ملفات الكمبيوتر.

٢-٧-١ تحرير بياناتك الشخصية من مكان إلى آخر (Passing your personal data around)

إذا كنت قد أعطيت كل هذه البيانات ، فأين هى الآن ؟ هل تم نقلها إلى جهة أخرى ؟ هل تم تأجيرها ؟ بيعها ؟ من الذى اطلع عليها ؟ هل يمكنك الوصول إليها ثانية ؟ أو بعبارة مختصرة أكثر صراحة ، هل بقى شىء خاص بك ؟

الحقيقة أنه - فى عصر المعلومات المحيكنة وخطوط الاتصال فائقة السرعة - يسهل جدا نقل بياناتك من كمبيوتر الى كمبيوتر ومن شبكة الى شبكة .. ومن ثم تصعب - وربما تستحيل - معرفة أماكن وجود بياناتك فى أى وقت لاحقه لإدلائك برأى .

ويتم نقل البيانات الشخصية لأسباب كثيرة .. فمثلا فى الولايات المتحدة ينقلون بيانات الأفراد من سجلات "خدمة الايرادات الداخلية للدولة "

[Internal Revenue Service (IRS)]

إلى سجلات الخدمة العسكرية لضبط المتخلفين عن التجنيد ، وكذلك إلى سجلات قروض الطلاب لمعاقبة من لم يلتزم منهم بالسداد .. ويثير تمرير البيانات من مكان الى آخر على هذا النحو جدلا واسعا على المستويين الرسمى والشعبى .

وفى بعض الأحيان ينجح الرأى العام فى منع تداول البيانات الشخصية .. حدث أنه أعلنت شركة خاصة عن قرب طرح أقراص مدمجة (CD - ROM) فى الأسواق تحتوى على بيانات كاملة عن كل مواطن أمريكى ، وأثار هذا الاعلان موجة عاتية من الاحتجاج والسخط اضطرت معها الشركة إلى إلغاء مشروعها .

ومع ذلك يسيطر القلق على الناس لاعتقادهم أنه أى بيان يخصهم - مهما كانت درجة سريته - سيجد طريقا عبر المسالك والبوّابات الكمبيوترية إلى من يدفع الثمن .. وفى محاولة لإعادة الاحترام ورد

الاعتبار لخصوصية الانسان التي انتهكها الكمبيوتر، بدأت التشريعات القانونية تقول كلمتها.

٢-٧-٢ قوانين حماية الخصوصية (Privacy legislation)

لجأت معظم الدول إلى وضع قوانين حماية الخصوصية لإشاعة جو الطمأنينة بين مواطنيها.. ونشير الى القوانين الخمسة الآتية المعمول بها في الولايات المتحدة:

(أ) قانون تصحيح بيانات الذمة المالية (Fair Credit Reporting Act)

ظهر هذا القانون عام ١٩٧٠ وهو يعطي المواطن الحق في معرفة تفاصيل سجلات ذمته المالية والاعتراض عليها إذا لم تكن صحيحة.. فهذه السجلات يتم إيداعها في ملفات الكمبيوتر بعد استيفاء بنودها من مصادر متعددة بعيدة عن ذهن المواطن العادي، وكان الناس يفاجأون بقرارهم بإعطاء بيانات مضللة عن مواقفهم المالية وهم لا يعرفون - وليس لهم أن يعرفوا - أسباب هذا القرار.. أما الآن فللأي مواطن الحق في الاطلاع على ما تم جمعه عنه من معلومات تتعلق بوضعه المالي للتأكد بنفسه من صحتها ودقتها، وله أن يصحح ما قد يجده من بيانات مخالفة لحقيقة الوضع.

(٢) قانون حرية المعلومات
(Freedom of Information Act)

ظهر هذا القانون أيضا عام ١٩٧٠ وهو علامة بارزة في تشريعات حماية الخصوصية ، وينص على أنه للمواطن العادي الحق في الاطلاع على جميع المعلومات التي تجمعها عنه الهيئات الرسمية الفيدرالية (وإن كان الكشف عن المعلومات يحتاج في بعض الأحيان الى حكم قضائي) .

(٣) قانون الخصوصية الفيدرالي
(Federal Privacy Act)

ظهر هذا القانون عام ١٩٧٤ ويعتبر أكثر القوانين تأثيرا في مجال حماية خصوصية الأفراد ، إذ يرسي مبدأ قانونيا هاما : "يجب ألا تكون هناك أية ملفات سرية عن المواطنين" .. فكل مواطن مسموح له بمعرفة ما يخصه من بيانات مخزونة في ملفات كمبيوترية أينما تكون ، وله أن يعرف الأغراض التي تستخدم فيها هذه البيانات ، كما أن له تصحيحها مكفول له على الدوام .

ويقضي القانون كذلك بأن تعلن الهيئة التي تجمع بيانات شخصية عن المواطنين مبررات مقنعة للقيام بهذا العمل ، وأن يكون المواطن على علم مسبق بذلك .

(٤) قانون حماية خصوصية التسجيلات المرئية
(Video Privacy Protection Act)

ظهر هذا القانون عام ١٩٨٨ وهو يمنع تداول

التسجيلات المرئية (الفيديو) الخاصة بالأشخاص إلا بعد موافقتهم .. ويطالب أنصار الخصوصية بتعميم ذلك على الملفات الطبية وملفات التأمين .

(٥) قانون المضاهاة بالكمبيوتر وحماية الخصوصية (Computer Matching and Privacy Protection Act)

ظهر هذا القانون عام ١٩٨٨ وهو يمنع الهيئات الحكومية من مقارنة ملفات الشخص المختلفة بقصد المضاهاة .. (ومع ذلك فعمليات المقارنة لازالت تجرى بدون تنظيم حقيقي) .

٢-٧-٣ الخصوصية في مواقع العمل (Privacy in the workplace)

بالرغم من أن العاملين لا يتوقعون أن يتمتعوا بخصوصية كاملة وهم في مواقع عملهم ، إلا أنهم عادة يصابون بصدمة كبيرة عندما يكتشفون أنهم واقعون تحت مراقبة رئيسهم ، وتعلو أصواتهم : "لابد من القضاء على هذا التجسس" .. والحقيقة أن رئيس العمل لا يقصد بالتجسس على العاملين ، ولكنه يدير مؤسسته بإمكانيات الكمبيوتر المتقدمة .

وقد اهتم المقاسم القانوني حول هذه النقطة بظهور "برامج المراقبة" (Surveillance software)

المصممة خصيصًا لمتابعة أعمال الموظفين من كل مكان بالمؤسسة .. فبضغطة بسيطة على مفتاح الفأرة (Mouse) يستطيع الرئيس أن يرى أمامه ماهو ظاهر في أي وقت على شاشة أي موظف أثناء أداء عمله.

وليس الأمر قاصرا على رؤية شاشات الموظفين عن بعد، ولكنه برامج المراقبة قادرة أيضا على مراجعة رسائل البريد الالكتروني لكل موظف، ومعرفة عدد ضرباته في الدقيقة على لوحة المفاتيح، ورصد طول فترة استراحته، وتحديد الملفات التي تعامل معها والمدة التي استغرقها هذا التعامل.

وتندد اتحادات العمال ببرامج المراقبة، وتقول إنه العاملين الذين يقعون فريسة "للتجسس" يعانون من ضغوط نفسية تفوق طاقة احتمالهم .. ولكن شركات انتاج برامج المراقبة تجزم بأن هذه البرامج ليست للتجسس، وإنما هي اليد اليمنى للرئيس في إدارة أعماله بأسلوب عصري.

وبذلك أنصار الخصوصية جهودهم في سبيل فرض ضوابط على عمليات المراقبة في مواقع العمل، ويحاولون استصدار قانون يعطي العاملين الحق في تنبيه زميلهم عندما يسلط عليه رئيسه عين المراقبة الكمبيوترية.

٢-٨ الاعتبارات الأخلاقية (Ethics)

في مجال العمل الكمبيوتري نرى ونسمع كل يوم

كثيراً من قصص المخالفات والتجاوزات الضارة بالعمل
ولا تكمن في الواقع إلا أخلاقيات الانسان :

• فتشاهد شخصاً يتعامل مع الديسكيتات في مكان عمله باستهتار ورعونة ، وقد يترتب على ذلك تلف ديسكيتات زاخرة بملفات البيانات .. والبيانات - كما علمنا - هي المورد (Resource) الحيوي الذي يصعب جداً - وربما يستحيل - إصلاحه أو استبداله .

• وتسمع عن موظف يتعمد البحث خلسة في ملف الأجور (Payroll file) ليعرف راتب زميل له لا يرغب في إطلاعه عليه .. وقد يصل التلصص على البيانات - مع شخص فاقد الضمير والقيم - إلى حد بيع أسرار عسكرية قومية إلى جهات أجنبية .

• وتفاجأ بأحد أصدقائك وقد واتته الجرأة لكي يضعك في موقف حرج ويطلب منك "استعارة" كلمة السر الخاصة بالعمل على كمبيوترات معمل كليتك .

• وتصدم في طالب زميلك في معاني الأمانة والشرف ، ودبّر خطة لاختراق حواجز أمن المنظومة الكمبيوترية في الكلية واستطاع تغيير درجات امتحانات بعض المواد له ولأصدقائه المتواطئين معه .

• وربما تكون اعتدت - بحكم المناخ المحيط - على نسخ البرامج دون أن تكلف نفسك التفكير فيما إذا كان هذا النسخ مشروعاً أم غير مشروع .. والحقيقة أن أخطر القضايا الأخلاقية الكمبيوترية هي تلك التي تتعلق بالنسخ غير القانونية (Illegal copies) التي

انتشرت - للأسف - على نطاق واسع من كل مكان ، وتعج مشكلات متفاقمة تشتد بالشكوى منها جميع الشركات الكبيرة و الصغيرة على السواء .. وتفرد لها هنا مناقشة مستقلة ..

٢-٨-١ نسخ البرامج (Copying software)

لم يعد مستغربا أن يتم تصوير جزء من كتاب أو الكتاب بأكمله على ماكينة تصوير مستندات وكذلك نسخ شرائط الأغانى وما شابهها على أجهزة التسجيل .. ورغم أن العمليه - تصوير الكتب ونسخ الأغانى - مخالفه للقانون ، إلا أنه يتكرر حدوثهما كل يوم ونادرا ما يقع الفاعل تحت طائلة القانون .. وبأسلوب لا يختلف كثيرا يتم نسخ برامج الكمبيوتر على اختلاف أنواعها ، ولكنه المخالفة فى هذه الحالة تنطوى على عواقب أخطر : فعملية تصوير كتاب تحتاج لمجهود ووقت وصورة الكتاب لا تكون أبدا فى نفس جودة الكتاب الأصلى ، أما نسخ برامج الكمبيوتر فعملية يسيرة وخيط تخرج نسخة البرنامج مطابقة تماما للأصل البرنامج وتؤدى وظيفته بنفس الدرجة من الكفاءة .. هذا بالاضافة الى الاعتبار المادى الرابح ، فنسخ شريط أكثر الأغانى نجاحا ورواجا لا يكلف الشركة المنتجة (والفنانه) أكثر من عشرة جنيهات ، أما نسخ برنامج كمبيوترى فقد يكلف الشركة المنتجة (والمبرمج)

آلاف الجنيهات.

ويمكننا تقسيم البرامج هنا إلى ثلاثة أنواع :

(١) البرامج المجانية (Freeware)

وهى برامج يقوم بتصميمها متطوعون أو هواه ويتم توزيعها مجانا للجمهور .. وهذه البرامج مسموح بنسخها دون أية محاذير لأنه استخدام النسخ - بدلالة الأصول - لا يسبب خسارة لأحد.

(٢) برامج المشاركة (Shareware)

وهى برامج يرسلها مصمموها إلى المستخدمين مجانا أيضا، ولكنهم - أى المصممين - يطمعون فى أن يرسل لهم المستخدم - طواعية - مشاركة مادية كريمة إذا ثبتت له كفاءة البرنامج وفائدته .. ولا يوجد ما يمنع نسخ مثل هذه البرامج واستخدام النسخ بحرية تامة.

(٣) البرامج ذات حقوق التأليف و النشر

(Copyrighted software)

هذه برامج قيمة متعددة الأغراض ويتكلف تصميمها كثيرا مثل برامج قواعد البيانات وتنسيق الكلمات والجداول الممتدة (Spreadsheets) .. وهى تباع بأسعار مرتفعة، ويحظر نسخها إلا بموافقة الشركة المنتجة و التى تتمتع بحقوق التأليف و النشر.

ونسخ تلك البرامج بدون تصريح يعتبر سرقة ويطلق عليه أيضا وصف "قرصنة البرامج" (Software piracy)، لأن النسخ يحرم الشركة المنتجة (ومصممى البرنامج) من الأرباح المشروعة المتوقعة .. لاحظ أنه ترك الحبل على

الغارب لقراصنة البرامج يجعل تصميم البرامج عملا غير مجز لمن يتصدى له، وعليه يقل أو يتوقف إنتاج البرامج الجيدة الجديدة مما يعود بالضرر علينا جميعا — هل يستطيع كل واحد منا أن يصمم برامج تطبيقاته بنفسه ؟!

ومع ذلك ننوه إلى أنه ليست كل عملية نسخ برنامج جريمة سرقة وليس كل ناسخ قرصانا .. فبعد أن تشتري برنامجا ببضع مئات من الجنيهات، سيتبه تفكيرك حتما لما يلي :

- عمل نسخة بديلة للبرنامج لتشغيلها عند الطوارئ.
- نسخ البرنامج على القرص الصلب لاستخدامه بمرونة أكثر.
- الاحتفاظ بنسخة من البرنامج في مكان عملك ونسخة أخرى في منزلك.

ومعظم المنتجين لا يلقون بالا لعمليات النسخ التي من هذا القبيل .. ولكن هناك آلافا من مستخدمي الكمبيوتر يحترفون النسخ لسبب آخر ومختلف تماما : الحصول على البرامج بدون دفع ثمنها .. وهنا تكمن المشكلة.

٢-٨-٢ محاربة نسخ البرامج
(Fighting software copying)

كرست شركات انتاج البرامج جهودها للتغلب على مشكلة نسخ البرامج، ونشير هنا إلى ثلاثة حلول مختلفة :

(١) وسائل منع النسخ (Copy protection)

لجأت الشركات في البداية إلى "وسائل منع النسخ"

التى تجعل البرامج تخرج من الشركة وهى غير قابلة للنسخ.. ولكنه قوبل هذا الحل بمعارضة قوية من مستخدمى الكمبيوتر على أساس أنه منع النسخ نهائيا عقاب للمذنبين والأبرياء أيضا أو - بعبارة أخرى - مضايقة جميع الشركاء من أجل مطاردة حفنة من اللصوص.. وتحت الضغط الجماهيرى أقلعت الشركات عن هذا الاجراء.

(٢) تصريح الموقع (Site licensing)

تتبنى بعض الشركات أسلوب "تصريح الموقع" والذى يعنى عقد اتفاقه مع العميل (موقع عمل) بموجبه يصرح له بنسخ برنامج (اشتراه من الشركة) أى عدد من المرات يشاء، واستخدام جميع العاملين للنسخ بحرية كاملة فى مختلف مراحل العمل.. ويكون التصريح مقابل مبلغ إضافى من المال يوافق عليه الطرفان.

(٣) التصريح الآنى (Concurrent licensing)

تلجأ شركات أخرى - فى مقدمتها شركة "ميكروسوفت" (Microsoft) الشهيرة - الى أسلوب "التصريح الآنى" وهو نظام يقدر المقابل المالى لتصريح نسخ البرامج على أساس عدد المستخدمين للبرنامج فى آنه واحد (ساعة ذروة العمل مثلا).. فمثلا أنه ٣٠ موظفا يعملون على شبكة كمبيوترية باحدى المؤسسات، ولكنه ١٠ منهم فقط هم الذين يستخدمون برنامج "ميكروسوفت إكسل" (Microsoft Excel) فى نفس الوقت فى مرحلة عمل معينة.. عندئذ تدفع المؤسسة ثمن ١٠ نسخ من البرنامج للشركة المنتجة.